

UNITED STATES DISTRICT COURT

FILED
ASHEVILLE, NC

AUG 09 2019

for the

Western District of North Carolina

U.S. DISTRICT COURT
W. DISTRICT OF N.C.

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*INFORMATION ASSOCIATED WITH DISCORD USER
ALLENWNC#8466 THAT IS STORED AT PREMISES
CONTROLLED BY DISCORD, INC.

Case No. 1:19 mj 70

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A of Attached Affidavit

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B of Attached Affidavit

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

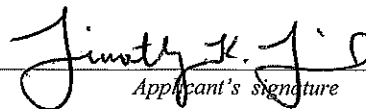
The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 2251(a)	Production of child pornography
18 U.S.C. § 2252A(a)(5)(B)	Possession of child pornography
18 U.S.C. § 2252A(a)(2)	Receipt and distribution of child pornography

The application is based on these facts:

See Search Warrant Affidavit

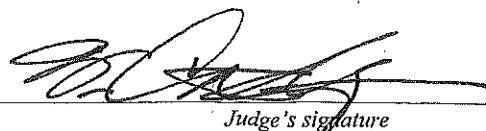
- ☒ Continued on the attached sheet.
- ☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

Timothy K. Thiel, Task Force Officer, HSI

Printed name and title

Sworn to before me and signed in my presence.

Date: 8/9/2019City and state: Asheville, North Carolina

Judge's signature

W. Carleton Metcalfe, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
DISCORD ACCOUNT ALLENWNC#8466
THAT IS STORED AT PREMISES
CONTROLLED BY DISCORD, INC.

Case No. _____

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Timothy K. Thiel, a Task Force Officer (TFO) with Homeland Security Investigations (HSI), being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a Task Force Officer (TFO) with the United States Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI). I am currently assigned to HSI Hendersonville, North Carolina office. As part of my official duties, I have conducted and participated in investigations related to cyber-crimes and the sexual exploitation of children. I have also received training and instruction in the field of investigating cyber related and child pornography crimes. I further have extensive experience in investigating cyber child exploitation cases to include the production, distribution, and transportation of child pornography images and videos via the internet. As part of my duties and responsibilities as an HSI Task Force Officer, I am authorized to investigate crimes involving the sexual exploitation of children pursuant to Title 18, United States Code, Section 2251, et seq.

2. This affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in **Attachment A** of this Affidavit, including the contents of the Discord user account username ALLENWNC#8466 (herein after referred to as SUSPECT USER ACCOUNT) that is stored at the premises owned, maintained, controlled, or operated by, Discord, Inc. located at 444 De Haro Street Suite 200, San Francisco, California 94107 94010. Discord is a company that provides remote computing and electronic communications services. This affidavit is made in support of an application for search warrant to look for contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2251, 2252, and 2252A, which items are more specifically described in **Attachment B** of this Affidavit.

3. The statements in this affidavit are based in part on information provided by other law enforcement investigators and on my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, § 2252A(a)(1), transportation of child pornography, Title 18, United States Code, § 2251(a) production of child pornography, Title 18, United States Code, § 2252A(a)(5)(B), possession of child pornography, Title 18, United States Code, § 2252A(a)(2) receipt and distribution of child pornography, are presently located in the SUSPECT USER ACCOUNT.

JURISDICTION

4. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. § 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court for the Western District of North Carolina: is “a district court of the United States . . . that has jurisdiction over the offense being investigated.”

DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment B:

a. “Anime,” as used herein, refers to refers to Japanese-style cartoon animation that is characterized by colorful graphics, vibrant characters, and fantastical themes, which may or may not include depictions of minors engaged in sexually explicit conduct.

b. “Chat,” as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

c. “Chat room,” as used herein, refers to the ability of individuals to meet in one location on the Internet in order to communicate electronically in real-time to other individuals.

Individuals may also have the ability to transmit electronic files to other individuals within the chat room.

d. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

e. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

f. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

g. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks,

external hard drives, “thumb,” “jump,” or “flash” drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

h. “Computer Server” or “Server,” as used herein, is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user’s computer via the Internet. A DNS (domain name system) server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol (IP) address so the computer hosting the web site may be located, and the DNS server provides this function.

i. “Computer software,” as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

j. “Computer-related documentation,” as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

k. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or

data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

l. “File Transfer Protocol” (“FTP”) is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP, built on client-server architecture, uses separate control and data connections between the client and the server.

m. “Hash value” is a unique alpha-numeric identifier for a digital file. A hash value is generated by a mathematical algorithm, based on the file’s content. A hash value is a file’s “digital fingerprint” or “digital DNA.” Two files having identical content will have the same hash value, even if the file names are different. On the other hand, any change to the data in a file, however slight, will change the file’s hash value, even if the file name is unchanged. Thus, if two files have the same hash value, they are said to be identical, even if they have different file names.

n. “Hyperlink” refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

o. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices

on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

p. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

q. An “Internet Protocol address” or “IP address,” as used herein, refers to a unique number used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (ISPs) control a range of IP addresses. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

r. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

s. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

t. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal,

whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

u. A “storage medium” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

v. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

w. A “website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (“HTML”) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (“HTTP”).

DISCORD ACCOUNTS & SERVICES

6. Discord provides free hosting for registered users to set up, configure, and customize their own communication servers, as well as user text chat rooms. Discord is a web-based service which can be accessed via web browser or by installing an application for a Windows, iOS, or Android device. Users register for the service with an email address, username, and password; after registering users have access to all of Discords’ features, including voice calls and chat rooms. Discord is an instant messaging service that provides both text and voice communication as well as video chat. Discord conversation logs are saved to a “Chats” area in the

user's Discord account. Discord account users can link other social media and entertainment services to their Discord account and can automatically integrate features of those applications such as Google+. Discord stores identifying information (such as email address used to register an account and a history of IP addresses), and usage information (such as chat logs, login sessions, and device information). Discord also collects information from any third-party application linked to a user's profile. The user account for a Discord account is alphanumeric username, which is then combined with a pound symbol (#) as well as a string of 4 or 5 randomized numbers, producing a unique "tag." The tag is publicly visible on an account's profile and can be used for a variety of networking purposes inside of Discord, such as friend lists, server whitelists, and blocking other users.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO ACCESS WITH INTENT
TO VIEW, RECEIVE, DISTRIBUTE, OR POSSESS CHILD PORNOGRAPHY**

7. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who transport, distribute, receive, possess, and/or access with intent to view child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety

of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials or purchase childlike sex objects for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic

tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual “deleted” it.¹

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses (including e-mail addresses), and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if BULEY uses a portable device (such as a mobile phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in the SUSPECT USER ACCOUNT as set forth in Attachment A.

8. Individuals who would have knowledge about how to access a hidden and embedded chat site would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat, or chat rooms have forums dedicated to the trafficking of child pornography images. Individuals who

¹ See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because “staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology”); see also *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

utilize these types of forums are considered more advanced users and therefore more experienced in acquiring child pornography images.

a. Such individuals, especially those utilizing cryptocurrency, and those who may have more knowledge and access to networks of other child pornography collectors and distributors, may be utilizing the dark web to access and purchase child pornography.

9. Based on the following, I believe that Jeffrey Allen BULEY, utilizing the SUSPECT USER ACCOUNT, likely displays characteristics common to individuals who transport, distribute, possess or access with intent to view child pornography.

PROBABLE CAUSE

10. On Sunday, July 28, 2019, the Hendersonville Police Department was dispatched to a residence located in Hendersonville, North Carolina, within the Western District of North Carolina due to a report by the residents that their son had possibly been sexually exploited.

11. At the residence, it was reported by the minor victim's parents that minor victim one (MV1), their 13-year-old son, was having inappropriate and sexually explicit conversations with an adult male who is an instructor at the taekwondo academy that MV1 attends. The suspect was identified as Jeffrey Allen BULEY.

12. During the investigation, I discovered that MV1 was communicating with BULEY via an app called Discord.

13. On Sunday, July 28, 2019 MV1's mother reported that she was calling for MV1 to come upstairs because dinner was ready, but MV1 repeatedly did not answer her. MV1's mother stated that when she went upstairs to look for MV1, she found him in the bathroom with the door closed. MV1's mother stated that as she approached the bathroom door, she heard MV1 talking

as if he was on the telephone and heard another male's voice. MV1's mother stated she heard MV1 make a reference to sex toys and after hearing such, she became suspicious and knocked on the door. MV1's mother stated that MV1 quickly disconnected the call and put down the device he was using.

14. MV1's mother stated she began looking through the device and discovered that MV1 had been using Wi-Fi to make telephone calls.

15. MV1's mother also discovered the Discord app but saw that the most recent record had been deleted.

16. MV1's mother and father then went to MV1's desktop computer and opened the Discord app and located messages between MV1 and a user utilizing the screenname "allenwnc."

17. MV1 explained to his parents that the user utilizing the screenname "allenwnc" was actually Jeffrey Allen BULEY. MV1 also provided the email address "allenwnc@yahoo.com" as an email address used by BULEY.

18. MV1 stated he began communicating with BULEY via the Internet and apps around August 2018 (when MV1 was then 12 years old) and began communicating with BULEY on the Discord app around April 2019.

19. MV1 stated that while communicating with BULEY via the Discord app, and possibly other apps, BULEY and MV1 would exchange nude photographs of each other, focusing on each other's genitalia. MV1 also stated BULEY would make specific requests for nude photographs of MV1's genitalia and MV1 would send the requested photos to BULEY via the Discord app or other apps.

20. MV1 reported incidents where he was alone with BULEY and stated that BULEY had sexually molested him. MV1 stated BULEY watched him completely undress to the point where MV1 was fully nude. MV1 also reported that BULEY has exposed his penis to MV1 and began masturbating in front of him and then also touched MV1's penis and began masturbating MV1. MV1 reported that BULEY has also touched his penis on the outside of his clothing.

21. On July 28, 2019, I met with MV1's parents and seized three devices belonging to MV1, an Apple iPod touch, a Samsung laptop, and a Hewlett-Packard computer tower.

22. Utilizing a Department of Homeland Security U.S. Immigrations and Customs Enforcement Consent to Search form, MV1's mother consented to HSI TFO Thiel seizing and searching the items mentioned above.

23. On Monday, July 29, 2019 I accessed MV1's account on the Discord app and located the following messages which occurred on Sunday, July 28, 2019 between MV1 (using screen name "DVM") and BULEY (using screen name "allenwnc"):

24. DVM: sup mate (1:05PM)

25. allenwnc: I think we're both cleaning up at the same time (5:03PM)

26. DVM: No I'm waiting for u (5:04PM)

27. To get a bath

28. allenwnc: Okay I can pull over for like 5 minutes somewhere hold on (5:04PM)

29. DVM: Ok (5:04PM)

30. allenwnc: Ok go (5:08PM)

31. DVM started a call (5:08PM)

32. MV1 stated the call placed was a video chat between himself and BULEY. MV1 stated that he was in his bathroom, fully nude, sitting in the bathtub showing BULEY his penis. MV1 stated this was the first time that he has chatted with BULEY while in the bathtub and stated that he usually video chats with him when he is taking a shower. MV1 stated BULEY was in a vehicle and had pulled over on the side of the road to video chat with him. MV1 stated that BULEY was using some sort of cellular smart phone at the time.

33. MV1 stated that he and BULEY routinely video chat via the Discord app. MV1 stated that he and BULEY regularly show each other their penises, masturbate and ejaculate. MV1 stated there have been times when BULEY has directed him what to do or what he would like to see MV1 do on the video chat.

34. On July 30, 2019 BULEY was arrested for violations of North Carolina state law and during his interview BULEY stated that he utilized the Discord app to communicate with MV1.

SPECIFICS OF SEARCH AND SEIZURE OF DISCORD ACCOUNT

35. Information stored in connection with a Discord account may provide crucial evidence of the “who, what, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. Stored electronic communications, and other data retained by Discord, can indicate who has used or controlled the Discord account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, Discord logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated

with the logged IP addresses; investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Discord account access, use, and events relating to the crime under investigation. Last, Discord account activity may provide relevant insight into the Discord account owner's state of mind as it relates to the offense under investigation. For example, information on the Discord account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

36. Therefore, the account servers of Discord are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Discord, such as account access information, transaction information, and other account information.

37. Because the warrant will be served on Discord who will then compile the requested records at a time convenient to Discord, reasonable cause exists to support execution of the requested warrant at any time day or night.

LEGAL AUTHORITY

38. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711 and 18 U.S.C. § 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is a "district court of the United States . . . that – (i) has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

CONCLUSION

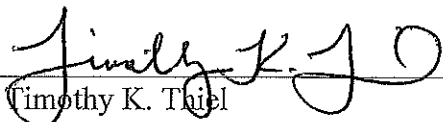
39. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that the Discord username ALLENWNC#8466 located on servers at Discord, 444 De Haro Street Suite 200, San Francisco, California 94107, have been used to distribute child pornography produced by the owner of the Discord account, in violation of 18 U.S.C. §§ 2251(a), 2252(a), and 2252A(a).

40. Further, there is probable cause to believe that evidence, fruits, and instrumentalities of such criminal offenses may be found in Discord records.

41. I, therefore, respectfully request that that attached warrant be issued authorizing the search and seizure of the items listed in **Attachment B**.

REVIEWED BY ASSISTANT UNITED STATES ATTORNEY DAVID A. THORNELOE

Respectfully submitted,



Timothy K. Thiel
Task Force Officer
Homeland Security Investigations

Subscribed and sworn to before me on August 8th, 2019


W. CARLETON MATCALF
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF LOCATIONS TO BE SEARCHED

This warrant applies to information associated with the Discord username ALLENWNC#8466 which is stored at premises owned, maintained, controlled, or operated by Discord, Inc. headquartered at 444 De Haro Street Suite 200, San Francisco, California 94107

ATTACHMENT B

PROPERTY TO BE SEARCHED AND/OR SEIZED

This warrant authorizes (i) the search of the property identified in Attachment A for only the following and (ii) authorizes the seizure of the items listed below only to the extent they constitute the following:

- (a) evidence of violations of 18 U.S.C. §§ 2252 and 2252A (“subject violations”); or
- (b) any item constituting contraband due to the subject violations, fruits of the subject violations, or other items possessed whose possession is illegal due to the subject violations; or
- (c) any property designed for use, intended for use, or used in committing any subject violations.

Subject to the foregoing, the items authorized to be seized include the following:

I. Information to be disclosed by Discord.:

To the extent that the information described in Attachment A is within the possession, custody, or control of Discord, including any emails, chats, images, records, files, logs, or information that have been deleted but are still available to Discord, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Discord is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all chats associated with the account, including stored or preserved copies of chats sent to and from the account, the source and destination addresses associated with each chat, the date and time at which each chat was sent, and the size and length of each chat;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between Discord, and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. All images depicting children engaging in sexually explicit conduct as defined in 18 U.S.C. § 2256

b. All electronic communications regarding children engaging in sexually explicit conduct;

c. All communications with potential minors involving sexual topics or in an effort to seduce the minor.

d. Any evidence that would tend to identify the person using the account when any of the items listed in subparagraphs a-c were sent, read, copied or downloaded.

e. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.